Comm...
rec'd 31 Jan '83

Comments on the DRAFT DCID 1/16 returned from the 18 Jan 1983 meeting.

Cover memorandum: Page 3, ADMINISTRATIVE REPORTS. Recommend text be changed from "...December detailing the accredited.." to "...December identifying the accredited..." Rationale: detailing implies exhaustive reports about all systems and networks under the NFIB member's jurisdiction. Within the IC, this could represent volumes of information unreadable by a horde of bureaucrats before the next report is due.

The following comments are directed at the DCI reg. xx-xx.

PAGE 5. Delete everything in Chapter I from paragraph I.2 to the end. Leave what is left in Chapter I as an Introduction only. Rationale: The generic security requirements described here are the same as those appearing in the DOD Computer Security Evaluation Center's DRAFT of Trusted Computer System Evaluation Criteria. The DRAFT TCSEC does not track well with the current or planned DOD or DCI regulations, and has not been formally accepted by the DOD or the Intelligence community as a useful tool.

PAGE 8. Change Chapter II to Chapter I. Rationale: see paragraph above.

PAGE 10. Office Information Systems. This paragraph does not quite meet the problem. The question that needs to be addressed, is what to do with "Office Information Systems"; "Office Automation Equipments"; and, "Personal Computers". Suggest that we need only identify the configuration, ie. "...any device with an instruction processor (CPU), and internal and/or external memory, used to process or store sensitive data." Any of these devices used to process or store sensitive data must meet the security requirements of the regulations. If the Word Processing equipments, or the Personal Computers are connected to an ADP system or network that is processing sensitive data, then the WP or PC must meet the security requirements for either terminals or other computer systems on the network. The bottom line, is forget about trying to delineate between what is a WP equipment, a Personal Computer, and an ADP system. Develop a set of security regulations that can be applied across the board without categorizing specific configurations.

PAGE 10, Paragraph II.9.a. Suggest change from "...a system knowledgeable individual" to "...the best technically competent individual available, with the appropriate security clearance...". Rationale: Persons knowledgeable about "systems" are not always knowledgeable about electronics maintenance. Suggest also adding a requirement for complete documentation about maintenance performed, components replaced, and review by fully cleared maintenance technicians. Replaced components from SCI systems should also be restricted from release from the classified facilities until sanitized or declared "clean" and unclassifed by competent technically qualified persons.

PAGE 10, Paragraph II.9.c. Remote diagnostic links should be permitted as long as they originate and terminate in fully cleared facilities, and are connected by secure communications. Rationale: Its already being done, and it is the state of the art.

PAGE 11, Chapter III, paragraph III.1. Change definition of Dedicated Mode to something that reads like "...specifically and exclusively dedicated and controlled for the support of one intelligence program or project, usually only requiring one level and type of clearance." Rationale: There are several computer installations already in operation, and adequately secured, that are devoted to a single mission. The computers are usually stand alone, and used by a small group of persons cleared and indoctrinated for all types of data used by the program or mission. To impose security requirements on these installations that are traditionally associated with the needs of general purpose computer systems, is costly and unreasonable.

PAGE 12, paragraph III.1.f. Footnote 1, definition for SCI does not seem to appear in the DRAFT DCID 1/16. Should appear here in any case. The DCI-reg is likely to be separated from the DCID in practice.

PAGE 12, paragraph III.2.b.(3) Use care to ensure that a requirement is not set that can be interpreted to mean that individual items of data must be be stored with appropriate security labels. Too costly. Classification of files of data, and the logic to default to the highest level when processing access requests will provide adequate security. When data is retrieved from an SCI computer system, exportable output media (ie. tape, disk, listing, etc.) should always be marked, even when unclassified. Unclassified is an appropriate classification when mixed with other classified data.

PAGE 13, PARA III.3.b.(1), and (4). Same objection as above.

PAGE 13, PARA III.3.b.(1) thru (6). All of these paragraphs start off with "Be capable of..". This terminology makes all of these requirements optional. Do we really want them to be optional, or are they "must be implemented" requirements?

PAGE 14, PARA III.3.c.(7). The last sentence in this paragraph should be removed. Rationale: This is a catch-22 requirement. Any and all code in any computer system, must by design place some level of dependence on other code. Even the nucleus of the Executive is dormant without external activity.

PAGE 14, PARA III.3.c(1). Change to read: "Only the NFIB member or his specific Designee can accredit an auto...". Rationale: Administrative continuity. If Designee can accredit other systems with data just as sensitive, this policy is inconsistent.

PAGE 14, PARA III.3.d(1). "Formal access approvals" and "need-to-know" criteria are mutually exclusive requirements. You can't have both. Just because a person works in the central computer facility, it may not be useful or necessary to brief these persons for all formal access programs. All persons working in the central facility need only be "cleared" for all types of sensitive data. For example, all persons must be cleared at the Top Secret level for all types of SCI processed, but need not be formally authorized access to special program accesses or "sub-compartments" within the overall SCI compartment.

PAGE 14, PARA III.3.d(2). Same discussion as above. "Formal access approval" versus "need-to-know".

PAGE 15, PARA III.4. Change name from "Expanded Compartmented Mode" to SCI/Collateral or Special Mode. Rationale: Expanded implies something bigger or better, when what is needed here is simply a mode to permit the mixing of SCI and Collateral data with a set of rules that insure reasonable security.

PAGE 15, PARA III.4, x.2.d(2)??? Same discussion here as above about the leading phrase "Be capable of...". Are these requirements optional?

PAGE 16, PARA III.4 (7). Last sentence of this paragraph should be removed.

PAGE 16, PARA III.4.c. Change the verbage to permit the NFIB member's specific Designee to accredit.

PAGE 16, PARA III.4.d(1). Formal access approval and need-to-know are mutually exclusive requirements.

PAGE 18, last paragraph. Add verbage to limit the life of an accreditation to no more than three years without review, or sooner if configuration changes are made that impact on the installed security.

Final comment. Where is the Glossary? Definition of the word access must be included. The current DCID 1/16 of 6 June 1978 definition of access is overly restrictive. Terminology needs to be included that will permit use of sensitive computers by persons not fully cleared through approved filter mechanisms.

STAT

[redacted]